UMEDA MASAO

FULL CONTENTS

[Claim(s)]
[Claim 1] The command-analysis section which analyzes the SCSI command, and the encryption mechanism which enciphers the writing data similarly extracted from the external file device number extracted in said command-analysis section, The decoding mechanism which was similarly extracted from the external file device number extracted in said command-analysis section and which reads and decrypts data, The equipment key management which manages the equipment key for every external file equipment, and the master key management which manages the master key of the whole file data encryption equipment, File data encryption equipment characterized by having the terminal control for control which controls the terminal for control which controls file data encryption equipment, and connecting with the SCSI interface section between a processing unit and external file equipment.
[Claim 2] Said master key is file data encryption equipment according to claim 1 characterized by being common to all pieces of the equipment connected to said SCSI interface.
[Claim 3] File data encryption equipment according to claim 1 characterized by having a means to specify the propriety of a code for every equipment as device-selector information.

[Detailed Description of the Invention]
[0001]
[Industrial Application] Especially this invention relates to the data code in the external file equipment connected with an SCSI interface about file data encryption equipment.
[0002]
[Description of the Prior Art] The conventional file cipher system handed over data from an user program or file input output device control to the code / decoding equipment by which external connection was carried out, as shown in drawing 3 , and it was performing the code/decoding of the data in a file.
[0003] Moreover, about management of the key, registration of an user program to a key, correction, and deletion were performed from the program with the independent key Management Department.
[0004] When a file code was performed from the beginning at the time of development of an user program, there was no problem in particular, but when it was going to add a file cryptographic function to an user program afterwards, change of the user program was required of the conventional technology.
[0005] It sets to delivery of the data between computer systems as a "data processing system" at JP,S56-47850,A. The method which realizes transmission and reception of the restricted data in each computer center is indicated by by computing the position in restricted data from the characteristic data and accompanying information of each computer center, and giving a code to the

position.
[0006]
[Problem to be solved by the invention] [when incorporating and developing a file code from the beginning to an user program in such a conventional file code, it was good, but] When already adding a file code to a certain user program, correction of the user program was required, when especially an user program was the third party's commercial program, it could not correct and there was a problem that a file cryptographic function could not be added as a matter of fact.
[0007] The [purpose of invention] The purpose of this invention is already enabling it to add a file cryptographic function without correction of the user program to a certain user program.
[0008]
[Means for solving problem] This invention is connected to the SCSI interface section between a processing unit and external file equipment as file data encryption equipment in order to solve said technical problem. The command-analysis section which analyzes the command for which file data encryption equipment needs encryption/decoding among the commands which pass SCSI, The encryption mechanism which enciphers the data on the SCSI command, the decoding mechanism which decrypts the data on the SCSI command, The encryption mechanism / decoding mechanism is equipped with the terminal control for control which controls the terminal for control for making input of a key, correction, etc. from the equipment key management which manages the key for every external file equipment, the master key management which performs the code/decoding of each whole equipment key, and the exterior.
[0009]
[Function] By inserting this by using a file code / decoding function as independent equipment between a processing unit and external file equipment, such as a floppy disk drive unit and CGMT equipment, according to this invention File encryption and a decoding function can be realized without completely correcting to the original user program.
[0010]
[Working example] Drawing 2 is the figure showing the topology of the file data encryption equipment of this invention, and the outline of a data flow.
[0011] In drawing 2 , an input/output is set to SCSI and enciphers only a part for the information bureau of writing data among the data from the PC/WC side. Moreover, it decrypts similarly about the data of an opposite direction.
[0012] To equipment, setup of the following information, change, deletion, etc. are performed from the exterior.
(1) Master key : it is common to all pieces of the equipment connected to an SCSI interface, and is the key for encryption of the cryptographic key for every equipment.
(2) Equipment key : it is the key which is connected to an SCSI interface and which is given for every equipment.
(3) Device-selector information : the propriety of a code can be specified for every equipment.
[0013] In addition, a setup of each information can be set up / changed with PC which let RS232C pass.
[0014] Moreover, although not specified in particular to a cipher system, when using a public key cryptosystem besides a conventional cryptosystem, a public key and the secret key for decoding are set as key information.
[0015] Drawing 1 is the outline block diagram of the file data encryption equipment of one working example of this invention.
[0016] In drawing 1 , the command-analysis section 1 analyzes the command group which flows on the SCSI interface of a processing unit and external file equipment, and extracts data read in other than the command for control, and the command for data write. When the writing data which accompanies the command when there is a command for data write is sent to the encryption mechanism 2 and there is a command for data read in, the read in data which accompanies the

command is sent to the decoding mechanism 3. At this time, the command-analysis section extracts an external file device number out of a command to data, and adds it to data.

[0017] The encryption mechanism 2 acquires the equipment key for through encryption for the equipment key management 4 from the external file device number sent from the command-analysis section, and performs a data encryption using this.

[0018] The decoding mechanism 3 acquires the equipment key for a through decoding for the equipment key management 4 from the external file device number sent from the command-analysis section, and decrypts data using this.

[0019] The equipment key management 4 holds the code / decoding key for every external file equipment connected to an SCSI interface.

[0020] Each equipment key is enciphered with one master key with this whole file encryption equipment. For this reason, if master keys differ even if it is the equipment key same between multiple-files data encryption equipment, it will become the key which differed also by the equipment key given identically.

[0021] The master key management 5 holds a master key peculiar to file data encryption equipment.

[0022] Although terminals for control, such as a personal computer connected to file data encryption equipment with RS232 C interface, to registration / change / deletion / reference are possible for a master key or an equipment key, the terminal control 6 for control controls this terminal for control.

[0023] In addition, when performing operation from the terminal for control, the security of operation is secured with a password.

[0024]
[Effect of the Invention] As explained above, this invention can encipher the file data in the external file equipment connected to the SCSI interface, without completely editing the existing user program.

[0025] Prevention of the data disclosure in the case of transmitting data, when external file equipment carries an actual medium by this by a removable medium thereby, for example becomes possible even when program modification usually uses the user program and utility program of difficult marketing.

[0026] Moreover, since this equipment is only added to the conventional system, it can use by any type-of-industry systems.

[0027] Moreover, since code propriety can be specified for every equipment, the same file form as usual can also be used.

[0028] Moreover, it is effective in especially the system information about is exchanged with the external system by the file.

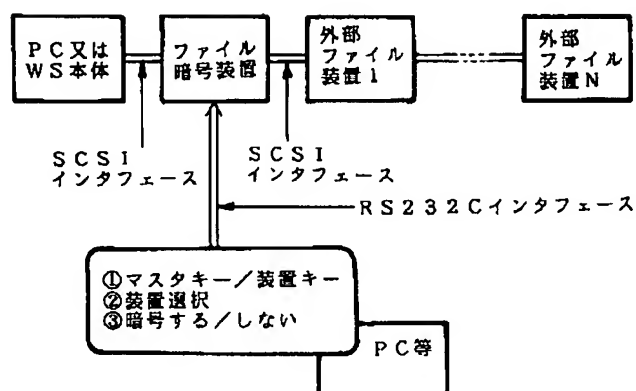
[Brief Description of the Drawings]
[Drawing 1] It is the block diagram of one working example of this invention.
[Drawing 2] It is the block diagram showing the topology of the file data encryption equipment of this invention.
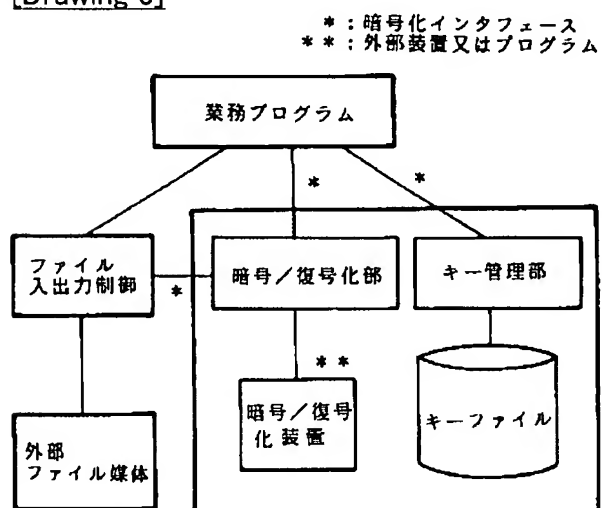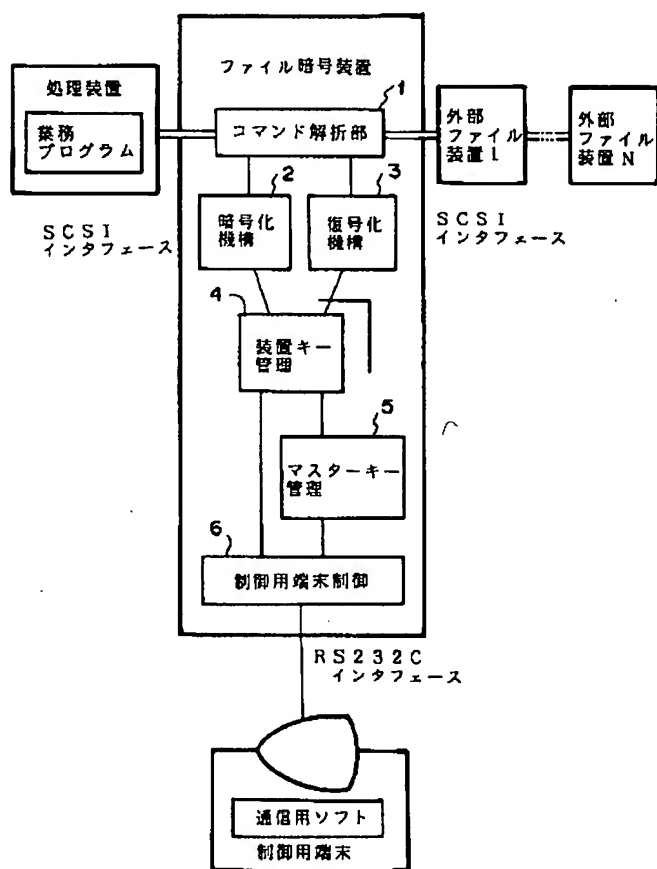[Drawing 3] It is the block diagram of the conventional file code / example of a decoding.

[Drawing 2]

```
┌─────┐   ┌─────┐   ┌─────┐          ┌─────┐
│PC又は│   │ファイル│   │外部  │          │外部  │
│WS本体│───│暗号装置│───│ファイル│──────────│ファイル│
│     │   │     │   │装置1 │          │装置N │
└─────┘   └─────┘   └─────┘          └─────┘
   │         │
SCSI       SCSI
インタフェース   インタフェース
   └───── RS232Cインタフェース

┌──────────────────┐
│①マスタキー／装置キー   │
│②装置選択          │
│③暗号する／しない     │───┐
└──────────────────┘   │
                  ┌─────┐
                  │PC等  │
                  └─────┘
```

[Drawing 3]

```
        ＊：暗号化インタフェース
        ＊＊：外部装置又はプログラム

         ┌──────────┐
         │ 業務プログラム  │
         └──────────┘
          ／    │＊    ＊＼
         ／     │       ＼
   ┌──────┐ ┌──────┐ ┌──────┐
   │ファイル  │ │暗号／復号化部│ │キー管理部 │
   │入出力制御 │＊│       │ │      │
   └──────┘ └──────┘ └──────┘
      │         │＊＊       │
   ┌──────┐ ┌──────┐ ┌──────┐
   │外部    │ │暗号／復号 │ │キーファイル│
   │ファイル媒体│ │化装置   │ │      │
   └──────┘ └──────┘ └──────┘
```

[Drawing 1]

[Translation done.]